

REMARKS

Firstly, Applicants object to the finality of the current Office Action. In particular, in the Office Action mailed May 4, 2005, the Examiner had finally rejected claims 1-11, 16 and 17 under 35 U.S.C. 103(a) as being unpatentable over Samar. In Applicants' response filed on July 15, 2005, Applicants had amended the claims and presented arguments over Samar. While this Amendment was not initially entered by the Examiner, it nonetheless was entered with the subsequent filing of an RCE. In response thereto, in the Office Action mailed January 3, 2006, the Examiner did not raise any art rejection, but rather rejected the claims under 35 U.S.C. 112, paragraph 2. In Applicants' response filed April 3, 2006, Applicants did not amend the claims but rather argued around the '112 rejection. Hence, Applicants submit that there is no reason for the current Office Action to be deemed "final".

The Examiner has finally rejected claims 16 and 17 under 35 U.S.C. 103(a) as being unpatentable over European Patent Application No. EP0752635A1 to Samar. Applicants acknowledge that the Examiner has allowed claims 1-11.

The Samar patent discloses a system and method to transparently integrate private key operations from a smart card with host-based encryption services, in which a computer 101 having a smart card reader 121 and an associated smart card 123 is connectable over a network 115 to a remote computer 119 or a

terminal 117 each having a smart card reader 121 and optionally an associated smart card 123. If the user of the computer 101 has a smart card 123 and inserts the same into the reader 121, the computer 101 enables the transmission of messages encrypted in accordance with the contents of the smart card 123. If no smart card is inserted, the computer 101 enables the transmission of messages encrypted in accordance with the contents of a user information file 127 and encryption services 129.

The subject invention relates to the transmission and reception of encrypted signals in, for example, a cable television system. In particular, at a headend, the cable provider encrypts a first signal in accordance with a first encryption scheme, and encrypts a second signal in accordance with a second encryption scheme. The cable provider then transmits both encrypted first and second signals. This is shown in Fig. 5, and in the specification on page 12, lines 10-13, where it is stated that the transmission station continually transmits the encrypted first and second signals.

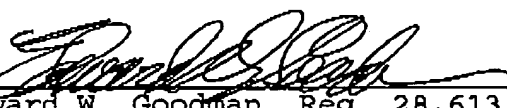
The invention, as claimed in claim 16, discloses encrypted transmissions of at least one signal, the first conditional access module only being able to decrypt a portion of the at least one signal which may then correspond to a first signal, and the second conditional access module being able to decrypt the whole of the at least one signal, which may then correspond to a second signal.

With regard to Samar, the encryption scheme being used to encrypt a signal being sent to the computer already takes into consideration whether or not the computer has a smartcard inserted therein. At no time does Samar disclose or suggest the transmission and reception of a signal in which a first conditional access module is only able to decrypt a portion of the signal, while the second removable conditional access module is able to decrypt the whole of the signal.

In view of the above, Applicants believe that the subject invention, as claimed, is not rendered obvious by the prior art, and as such, is patentable thereover.

Applicants believe that this application, containing claims 1-11, 16 and 17, claims 12-15 having been withdrawn, is now in condition for allowance and such action is respectfully requested.

Respectfully submitted,

by 
Edward W. Goodman, Reg. 28,613
Attorney
Tel.: 914-333-9611